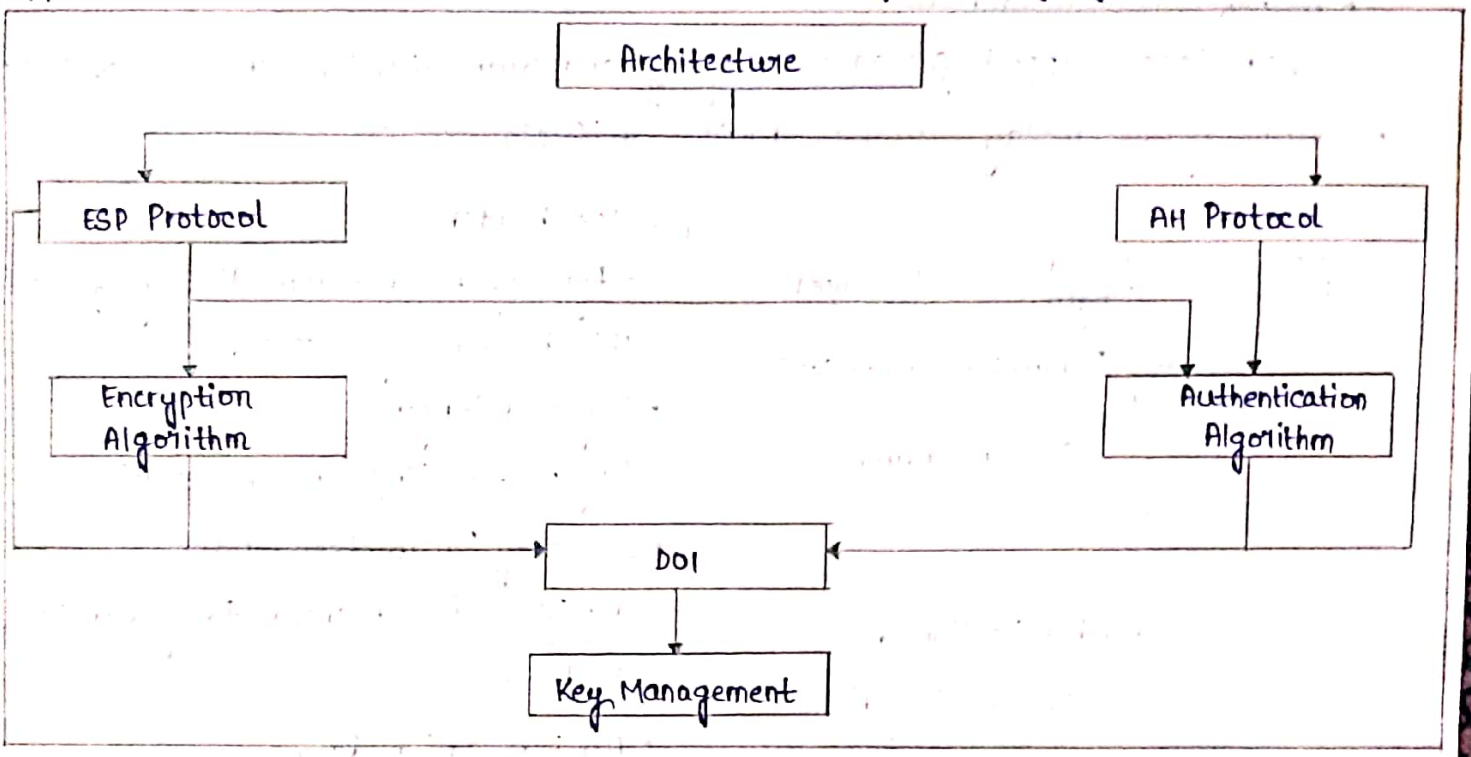
18311A12J6
P. Akshitha Reddy

INFORMATION SECURITY ASSIGNMENT-2

UNIT-4

1. Briefly discuss about IP Security Architecture and also about AH and ESP protocols in detail.

Ans: Implements Security at the IP level. This ensures Secure networking not only for application with Secure mechanisms but also for many Security-ignorant applications.



IP Security Architecture

① Architecture: Architecture of IP Security Architecture Covers the general concepts, definitions, protocols, algorithms and Security requirements of IP Security technology.

② ESP Protocol: ESP (Encapsulation Security Payload) provide the Confidentiality Service. Encapsulation Security Payload is implemented in either two ways:

- ESP with optional Authentication.
- ESP with Authentication.

③ Encryption Algorithm: Encryption algorithm is the document that describes various encryption algorithm used for Encapsulation Security Payload.

④ AH Protocol: AH (Authentication Header) Protocol provides both Authentication and Integrity Service. Authentication Header is implemented in one way only: Authentication along with Integrity.

⑤ Authentication Algorithm: Authentication Algorithm Contains the set of the documents that describe authentication algorithm used for AH and for the

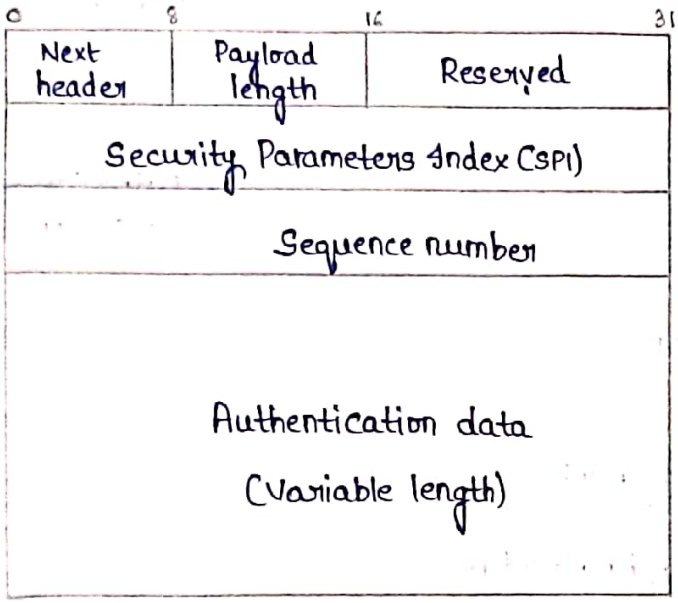
authentication option of ESP.

⑥ DOI (Domain of Interpretation): DOI is the identifier which support both AH and ESP protocols. It contains values needed for documentation related to each other.

⑦ Key Management: Key Management contains the document that describes how the keys are exchanged between sender and receiver.

→ Authentication Header - AH:

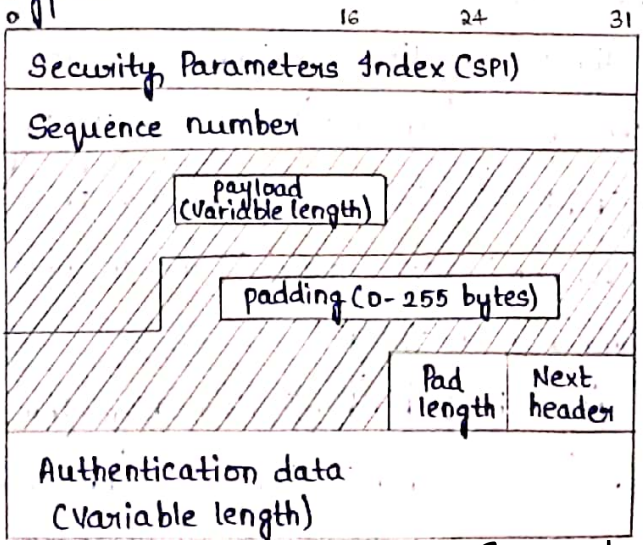
- provides support for data integrity and authentication (MAC code) of IP packets.
- Guards against replay attacks - provides antiReplay service.



- Next header
  - type of header immediately following this header (e.g., TCP, IP, etc)
- Payload length
  - length of AH (in 32 bit words) minus 2
- Security Parameters Index
  - identifies the SA used to generate this header.
- Authentication data
  - a (truncated) MAC or ICV (default length is ~~in~~ 3x32bits).

→ Encapsulating Security Payload (ESP):

- provides all that AH offers, and
- In addition provides data Confidentiality
  - uses Symmetric Key encryption.

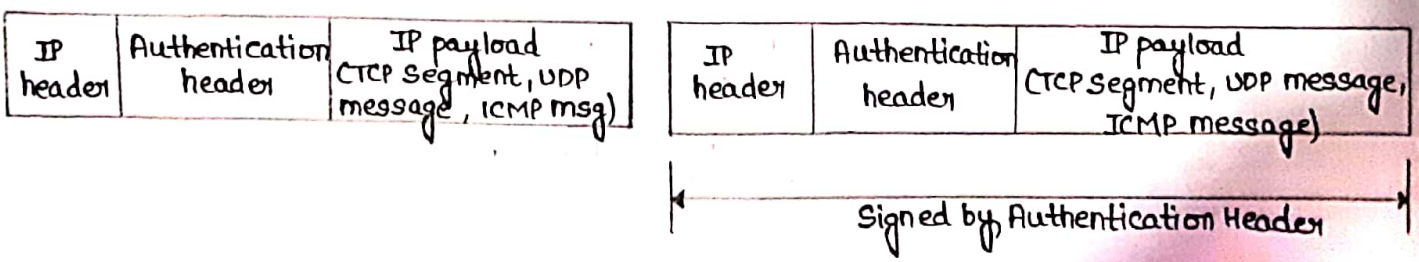


• Security Parameters Index
- identifies the SA used to generate this encrypted packet.
• Sequence Number
- Sequence number of the packet.
• payload
- transport level Segment (transfer mode) or encapsulated IP packet (tunnel mode)
• padding (0-255 bytes)
- Variable length padding
• pad length (8 bits)
• Next header
- identifies the type of data contained in the payload.
• Authentication data
- a (truncated) MAC computed over the ESP packet (SPI ... Next header).

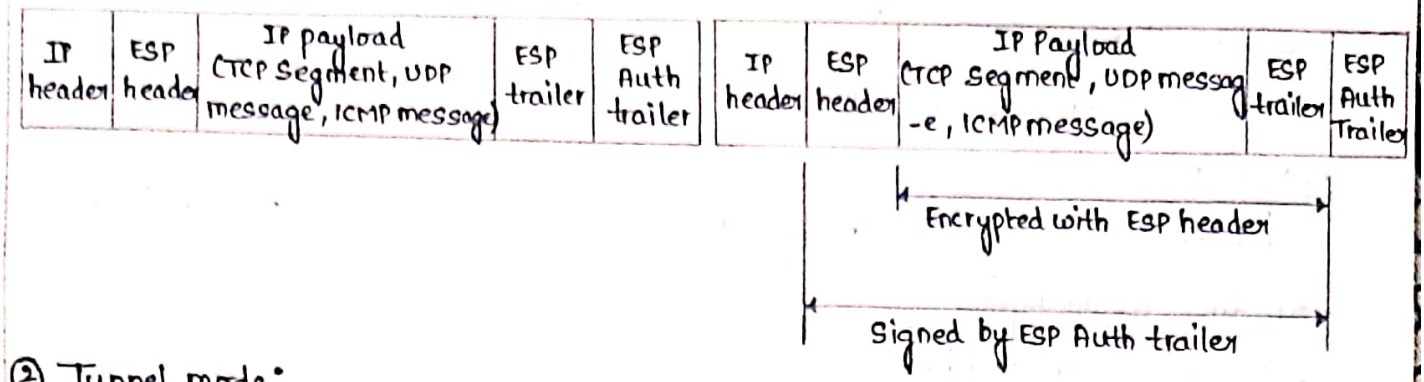
2. What are the H Combinations of Security Associations in IP Security.

Ans: • A one-way relationship between a sender and a receiver system.
• Used either for AH or for ESP but never for both.
• Modes of operation - transport and tunnel mode
-purpose of modes of operation: Interoperability

① Transport mode:
- default mode
- provides protection primarily for upper layer protocols.
- usually used between end-systems.
- protection is applied to the payload of the IP packet
• AH in transport mode authentication the IP payload and selected fields of the IP header.

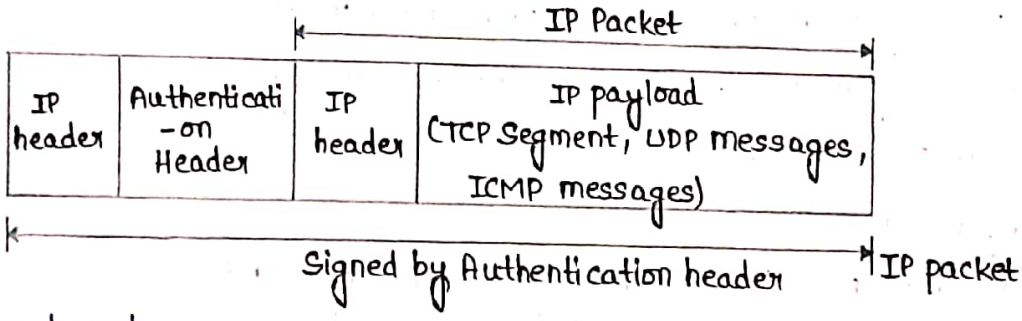


• ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.

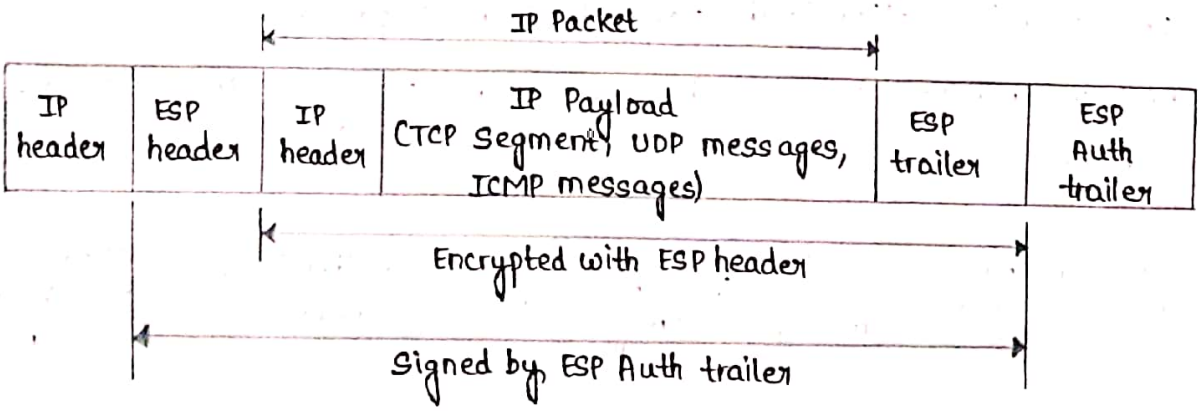


② Tunnel mode:

- usually used between Security gateways (routers, firewalls) for interoperability like Gateway-to-gateway, Server-to-gateway, Server-to-Server.
- useful for protecting traffic between different and untrusted networks.
- provides protection to the entire IP packet.
- the entire IP packet is considered as payload and encapsulated in another IP packet (with potentially different source and destination addresses).
• AH in transport mode authenticates the entire inner IP packet and selected fields of the outer IP header.



• ESP in tunnel mode end.



UNIT-5

1) Differentiate between SSL and TLS?

Ans: SSL Stands for Secure Socket layer while TLS Stands for Transport layer Security. Both Secure Socket layer and Transport layer Security are the protocols used to provide the Security between web browser and web server.

Secure Socket Layer (SSL)	Transport Layer Security (TLS)
① SSL Stands for Secure Socket layer.	① TLS Stands for Transport layer Security.
② SSL (Secure Socket layer) Supports Fortezza algorithm.	② TLS (Transport layer Security) does not Supports Fortezza algorithm.
③ SSL (Secure Socket layer) is the 3.0 version.	③ TLS (Transport layer Security) is the 1.0 version.
④ In SSL, Message digest is used to create master secret.	④ In TLS, Pseudo-random function is used to create master Secret.
⑤ In SSL, Message Authentication Code protocol is used.	⑤ In TLS, Hashed message Authentication code protocol is used.
⑥ SSL is Complex than TLS (Transport layer Security).	⑥ TLS (Transport layer Security) is Simple.
⑦ SSL is less Secured as Compared to TLS (Transport layer Security).	⑦ TLS (Transport layer Security) provides high Security.

2) Explain in detail about payment processing in SET.

Ans: SET is an open encryption and security specification designed to protect credit card transactions on the Internet.

Payment processing:

Purchase Request: Message from Customer to merchant Containing OI for merchant and PI for bank.

- Before the purchase request exchange begins, the Cardholder has Completed browsing, Selecting, and ordering.

• The purchase request exchange consists of four messages: Initiate Request, Initiate Response, Purchase Request, and Purchase Response.

• Initiate Request message: The customer requests the certificates (merchant and payment gateway) to the merchant.

• The Initiate Response message: Merchant responds with his certificates and payment gateway.

• Next, the cardholder prepares the purchase Request message.

• Purchase Request message includes the following:

① Payment-related information ② Order-related information ③ Cardholder certificate.

• When the merchant receives the purchase Request message, it performs the following

① verifies the cardholder

② Forwards the payment information to the payment gateway for authorization.

③ Sends a purchase response to the 'Cardholder.

• The Purchase Response message = $DS(KR_M$, response block that acknowledges the order)

• When the Cardholder receives the purchase Response message, it verifies the signature on the response block.

Payment Authorization:

Exchange between merchant and payment gateway to authorize a given amount for a purchase on a given Credit Card a/c.

• During the processing of an order from a Cardholder, the merchant authorizes the transaction with the payment gateway. This authorization guarantees that the merchant will receive payment. The merchant can therefore provide the services or goods to the customer.

• The payment authorization exchange consists of two message:
Authorization Request and Authorization Response.

• The merchant sends an Authorization Request message to the payment gateway consisting of

1. Purchase-related information = PI || DS || OIMD || Digital Envelope.

2. Authorization-related information

- Authorization block includes transaction ID
- A digital envelope.

3. Certificates
   - Cardholder's certificate
   - Merchant's Signature key Certificate
   - Merchant's key exchange Certificate

• The payment gateway performs the following tasks:

1. Verifies all certificates
2. Decrypts the digital envelope and decrypts the authorization block
3. verifies the Dual Signature.

• The payment gateway returns an Authorization Response message to the merchant includes the following:

1. Authorization - related information
   - Authorization block
   - Digital envelope.
2. Capture token information
3. Certificate
   - The gateway's Signature key Certificate.

Payment Capture:

• To obtain payment, the merchant engages the payment gateway in a payment capture transaction, Consisting of a capture request and a Capture response message.

• The Capture Request message includes the following:

- Capture request block = payment amount || transaction ID || Encrypted Capture token || Merchant's Certificates.

• When the payment gateway receives the Capture request message, it decrypts and verifies the Capture request block and verifies the Capture token block.

• It then sends clearing request to the issuer over the private network. This request Causes funds to be transferred to the merchant's account.

• The gateway then notifies the merchant of payment in a Capture Response message The message include the following:

- Capture response block
- gateway's Signature key Certificate.

UNIT-6

1. What is a Firewall? Discuss about Various firewalls and its principals?

Ans: Effective means of protecting a local system or network of systems from network-based security threats.

- Also afford access to the outside world via WANs and the Internet.

Types of firewalls:

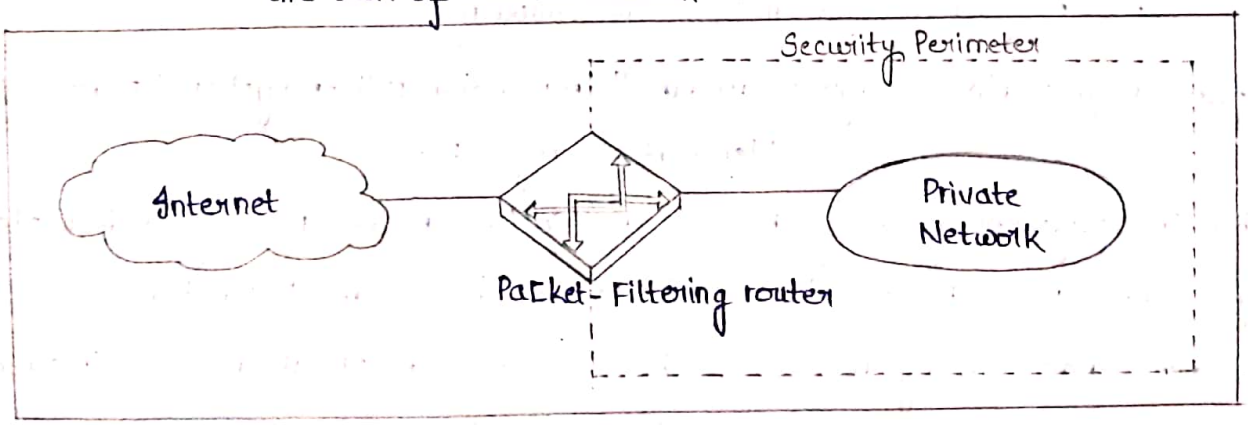
① packet-filtering router

② Application-level gateway

③ Circuit-level gateway.

① Packet-filtering router: It applies a set of rules to each incoming IP packet or outgoing IP packet and then forwards or discards the packet.

- Filtering rules based on fields in
  - IP and transport (e.g., TCP or UDP) header, including Source and destination IP address
  - IP protocol field, and
  - TCP or UDP port number
- Advantages: - Simplicity
  - transparent to users and are very fast
- Disadvantages: - Difficulty of setting up packet filter rules correctly
  - the lack of authentication.



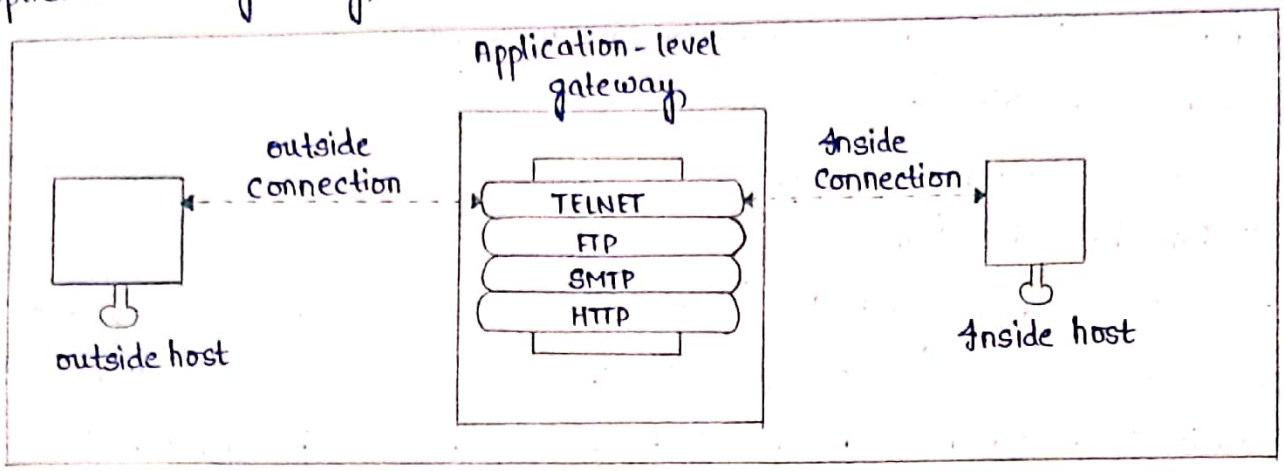
Packet-Filtering router

② Application-level Gateway: Also called a proxy server, acts as a relay of application-level traffic.

- The user contacts the gateway using a TCP/IP application, such as Telnet or FTP, and the gateway asks the user for the name of the remote host to be accessed.

• When the user responds and provides a valid user ID and authentication information, the gateway contacts the application on the remote host and relays TCP segments containing the application data between the end points.

• Application-level gateways tend to be more secure than packet filters.



Application-level gateway

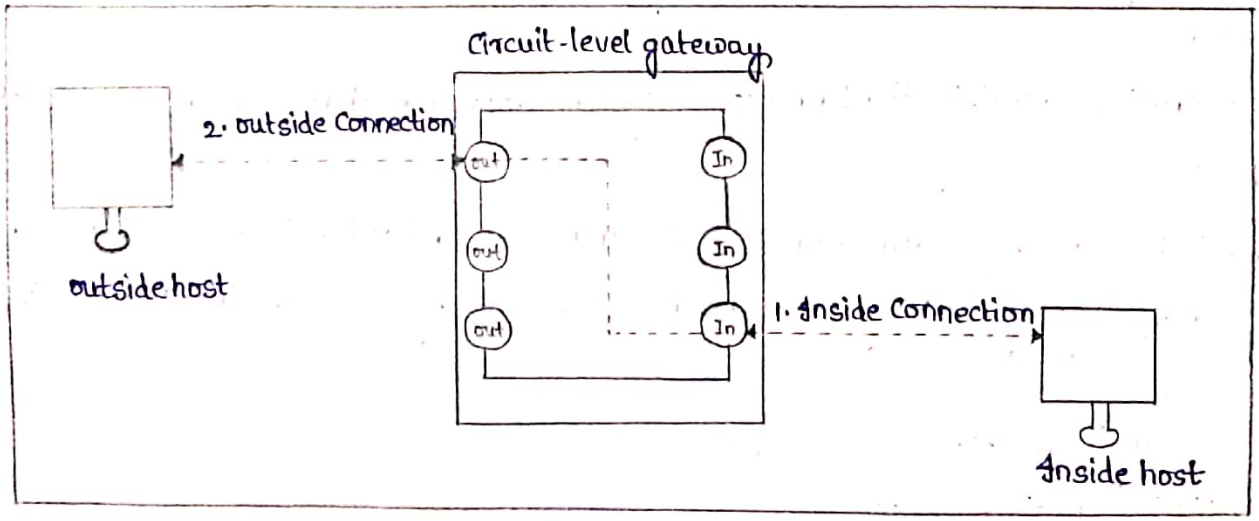
③ Circuit-level Gateway: This can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain functions.

• It does not permit an end-to-end TCP connection; rather, the gateway sets up two ~~Two~~ TCP connections,

1. between itself and a TCP user on an inner host and
2. between itself and TCP user on an outside host.

• Once the two connections are established, the gateway typically relays TCP segments from one connection to the other without examining the contents.

• Typical use: A system where system administrator trusts the internal users.



Circuit-level gateway.

2. Explain Intrusion Detection Systems.

Ans: ① If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised.

② Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

③ Intrusion detection approaches are:

(i) Statistical anomaly detection

(ii) Rule-based detection

(i) Statistical anomaly detection: Involves the collection of data relating to the behavior of legitimate users over a period of time. Then statistical tests are applied to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

- It has two categories:

- Threshold detection: This approach involves defining thresholds, independent of user, for the frequency of occurence of various events.

- Profile based: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

(ii) Rule-based detection: Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

- It has two categories:

- Anomaly detection: Rules are developed to detect deviation from previous usage patterns.

- Penetration identification: An expert system approach that searches for suspicious behavior.

④ Audit Records: A fundamental tool for intrusion detection is the audit record. Some record of ongoing activity must be maintained ~~on~~ by users as input to an intrusion detection system.

- Basically two plans are used:

(i) Native audit records

(ii) Detection-Specific audit records.